IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application for:

CONTENT SCRAMBLING WITH MINIMAL IMPACT ON LEGACY DEVICES

Inventor(s): James Bonan, Brant Candelore, and Mark Eyer

Docket Number: SNY-T5462.02

Prepared By: Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606

Phone: (919) 816-9981
Fax: (919) 816-9982
Email: miller@patent-inventions.com

CERTIFICATE OF EXPRESS MAILING FOR NEW PATENT APPLICATION

"Express Mail" mailing label number ER126259254US

Date of Deposit 1/29/04

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Catherine N. Miller
(Typed or printed name of person mailing paper or fee)

Catherine N. Miller
(Signature of person mailing paper or fee)

CONTENT SCRAMBLING WITH MINIMAL IMPACT ON LEGACY DEVICES

CROSS REFERENCE TO RELATED DOCUMENTS

This application claims priority benefit of U.S. Provisional Patent Application Serial No. 60/457,192, filed March 25, 2003, entitled "Content Scrambling with Minimal Impact on Legacy Devices", to Bonan, et al., which is hereby incorporated by reference. This application is also related to patent applications serial number 10/038,217; serial number 10/038,032; serial number 10/037,914; serial number 10/037,499; and serial number 10/037,498. These patent applications were filed simultaneously on January 2, 2002 and are hereby incorporated by reference herein.

COPYRIGHT NOTICE

BACKGROUND

Television is used to deliver entertainment and education to viewers. The source material (audio, video, etc.) is multiplexed into a combined signal which is then used to modulate a carrier. This carrier is commonly known as a channel. In terrestrial broadcasts, these channels correspond to government assigned frequencies and are distributed over the air. The program is delivered to a receiver that has a tuner that selects the signal from the air and delivers it to a demodulator, which in turn provides video to a display and audio to speakers.

Much of television content is valuable to its producers, therefore copyright holders want to control access, disallow re-transmission of content over the Internet, and restrict copies. Examples of such protected material include, but are not limited to, feature films and sporting events. Currently, television terrestrial broadcast systems do not generally use any sort of control measures such as encryption systems to prevent unauthorized copying of content.

DESCRIPTION OF THE DRAWINGS

The present invention, both as to organization and method of operation, together with objects and advantages thereof, may be best understood by reference to the following detailed description, which describes certain exemplary embodiments of the invention, taken in conjunction with the accompanying drawings in which:

FIGURE 1 is a block diagram of a conventional terrestrial broadcast system.

FIGURE 2 is a flow chart of a dual delivery and encryption process consistent with certain embodiments of the present invention.

FIGURE 3 is a flow chart of a dual delivery and encryption process consistent with certain embodiments of the present invention.

FIGURE 4 is a block diagram of a TV consistent with certain embodiments of the present invention.

FIGURE 5 is a block diagram of Broadcast Flag usage consistent with certain embodiments of the present invention.

DETAILED DESCRIPTION

While this invention is susceptible of embodiment in many different forms, there are shown in the drawings and will herein be described in detail specific embodiments, with the understanding that the present disclosure is to be considered as an example of the principles of the invention and not intended to limit the invention to the specific embodiments shown and described. In the

description below, like reference numerals are used to describe the same, similar or corresponding parts in the several views of the drawings.

The following acronyms and abbreviations may be used herein:

ATSC – Advanced Television System Committee

A/V – Audio / Video

CA - Conditional Access

CPU – Central Processing Unit

DMA – Direct Memory Access

DTV – Digital Television

ECM - Entitlement Control Message

EPG - Electronic Program Guide

FCC – Federal Communications Commission

HDD – Hard Disk Drive

MPEG - Moving Pictures Experts Group

PAT - Program Allocation Table

PID - Packet Identifier

PMT - Program Map Table

PSI - Program Specific Information

PVR – Personal Video Recorder (a digital disk based video recorder)

RAM - Random Access Memory

SDRAM – Synchronous Dynamic Random Access Memory

STB – Set Top Box

TV - Television

Critical Packet - A packet or group of packets that, when encrypted, renders a portion of a video image difficult or impossible to view if not properly decrypted, or which renders a portion of audio difficult or impossible to hear if not properly decrypted. The term "critical" should not be interpreted as an absolute term, in that it may be possible to hack an elementary stream to overcome encryption of a "critical packet", but when subjected to normal decoding, the inability to fully or properly decode such a "critical packet" would inhibit normal viewing or listening of the program content. The MPEG transport specification specifies 188 bytes per

packet. At the program stream level, packets may be variable in size, e.g., typically on the order of 2000 bytes.

Selective Encryption (or Partial Encryption) – encryption of only a portion of an elementary stream in order to render the stream difficult or impossible to use (i.e., view or hear).

Dual Selective Encryption – encryption of portions of a single selection of content under two separate encryption systems.

The terms "a" or "an", as used herein, are defined as one, or more than one. The term "plurality", as used herein, is defined as two or more than two. The term "another", as used herein, is defined as at least a second or more. The terms "including" and/or "having", as used herein, are defined as comprising (i.e., open language). The term "coupled", as used herein, is defined as connected, although not necessarily directly, and not necessarily mechanically. The term "program", as used herein, is defined as a sequence of instructions designed for execution on a computer system. A "program", or "computer program", may include a subroutine, a function, a procedure, an object method, an object implementation, in an executable application, an applet, a servlet, a source code, an object code, a shared library / dynamic load library and/or other sequence of instructions designed for execution on a computer system.

The terms "scramble" and "encrypt" and variations thereof may be used synonymously herein. Also, the term "television program" and similar terms can be interpreted in the normal conversational sense, as well as a meaning wherein the term means any segment of A/V content that can be displayed on a television set or similar monitor device. The term "video" is often used herein to embrace not only true visual information, but also in the conversational sense (e.g., "video tape recorder") to embrace not only video signals but associated audio and data. The term "legacy" as used herein refers to existing technology used for existing terrestrial broadcast systems. The exemplary embodiments disclosed herein can be decoded by a television Set-Top Box (STB), but it is contemplated that such technology will soon be incorporated within television receivers of all types whether housed in a separate enclosure alone or in conjunction with recording

and/or playback equipment or Conditional Access (CA) decryption module or within a television set itself.

A conventional broadcast system arrangement is depicted in **FIGURE 1**. At the broadcast station 10 in such a system, the broadcaster processes audio/video (A/V) content 14 in the clear. The A/V content along with system information (SI) 26 and program specific information (PSI) 27 is multiplexed together at multiplexer (MUX) 30, modulated and transmitted over the air via antenna 32 to a user's TV 36. TV 36 demodulates the signal and supplies it to a television set 44 for viewing by the user.

In a terrestrial system such as that of **FIGURE 1**, digital program streams are broken into packets for transmission. Packets for each component of a program (video, audio, auxiliary data, etc.) are tagged with a packet identifier or PID. These packet streams for each component of all programs carried within a channel are aggregated into one composite stream. Additional packets are also included to provide other overhead information.

Overhead information usually includes guide data describing what programs are available and how to locate the associated channels and components. This guide data is also known as system information or SI. In terrestrial broadcasts, SI is delivered to the television receiver or set-top box (STB) in-band (part of the data encoded within a channel).

The broadcast is received at a television (or STB) 40 via antenna 44 which passes the received signal to tuner 48 which translates the incoming signal to baseband or intermediate frequency. The receiver 52 then decodes the programming for display on the television display.

As of spring 2003, approximately 4.7 million High Definition (HD) -ready digital TVs (DTVs) have been produced and sold to consumers since the fall of 1998 in the U.S. About 11 percent, or 543,000, were sold with integrated DTV tuners. These sets, such as TV 40, cannot descramble content, should the terrestrial broadcasters choose to protect their content through scrambling, and might be rendered obsolete or in need of modification or in need of use of an adapter.

Enforcement of conditional access to protected content often involves scrambling that content in a cryptographically secure manner. Authorized devices have the hardware support for descrambling, and are given the decryption keys. Unauthorized devices may have the hardware, but will not generally have access to the keys necessary for descrambling.

Conditional access (CA) technology often involves use of intellectual property protected by patent or trade secret, therefore authorized devices are subject to the terms of a technology license. Terms of such licenses often involve provisions requiring protection of digital outputs appropriate to the "copy control information" (CCI) applicable to a given piece of content. The license may also require cryptographic keys and algorithms to be protected, to some degree, against physical attack. These provisions are called "robustness rules." If scrambling were to be used for terrestrial broadcast, then new TVs or other television receiver devices could be built to support the chosen method of conditional access (using conditional access modules or embedded keys necessary for descrambling). Access to the keys whether through conditional access or embedded keys could be subject to licensing terms. Part of the licensing terms could allow the broadcaster to enforce content handling rules. The moment terrestrial broadcast scrambling were switched on, however, legacy DTVs would be immediately impacted. They would be unable to access any scrambled services since they would lack the necessary descrambling circuitry and access to the keys.

The only known current option to avoiding letting the existing DTVs go dark is "full dual carriage". Full dual carriage means that transmission is duplicated for each program – it is sent in the clear and also sent encrypted. To provide full dual carriage, the broadcast stream is enhanced to provide encryption. Legacy TVs would not be impacted and would continue to perform their function despite any change. However, full dual carriage often comes at an unpalatable price because of the bandwidth impact, thus reducing the number of unique programs that a broadcaster may offer. In a simple case, "full dual carriage" would require the same bandwidth for both the "in the clear" and encrypted program streams. If the original unencrypted stream is using up all, or most, of the

available bandwidth (as would be the case with a High Definition broadcast), "full dual carriage" is clearly not an option. Thus, "full dual carriage" suggests that both program streams be carried at a substantially lower quality level, in order to fit in the available bandwidth. In simple terms, this would mean carrying the program stream at a lower quality level than in the pre-encrypted case. Generally, the number of premium channels suffers so that the number of options available to the viewer, and/or the quality of the program, is limited and the value that can be provided by the broadcasters is diminished.

The broadcaster may chose to leave the main channel in-the-clear so that it may be descrambled by both old and new TVs. Secondary channels may be fully encrypted and only available to new TVs. However, using secondary channels takes away from the overall bandwidth that may be used for the primary channel, as described above. Ideally, some method is needed to make old and new TVs work on the primary channel without wasting bandwidth, while at the same time allowing the broadcasters to protect their content.

Broadcasters wish to prevent unauthorized re-distribution of their content over the Internet. As of this writing, the ATSC standards organization has proposed the use of a "broadcast flag" with the standard A/65A, which would indicate that copyright is asserted for certain broadcast programming and that Internet distribution of broadcast programming labeled with this flag is disallowed. Proposed regulations related to the Broadcast Flag would require a mechanism to block unauthorized distribution beyond the personal digital network environment. The Broadcast Flag is a descriptor sent in the program specific information (PSI). It is anticipated by proponents of the Broadcast Flag, that legislation or FCC regulations would require television tuners and similar devices to comply with certain specification to prohibit unauthorized redistribution. However, the Broadcast Flag does not itself protect or encrypt content. Those functions are performed by the FCC regulations. As a result, the transmission remains in the clear, and subject to reception and unauthorized redistribution outside the United States, where FCC regulations do not apply or by those willing to defy such regulations in the United States.

A solution that allows the use of encryption would mitigate this problem, since tuners, even outside the scope of FCC regulation, would need to license decryption technology, which would include restrictions limiting unauthorized redistribution. To date, encryption solutions have not been widely believed to be acceptable solutions for three principal reasons: 1)the perceived bandwidth problems described above, 2) the inherent incompatibility with the installed base of DTV receivers, and 3) cessation of sales of current and near-term future DTV receivers that do not incorporate decryption.

The present invention provides a solution for these issues. By enabling the simultaneous transmission of both in-the-clear, and encrypted signals, without significant additional bandwidth requirements, the invention enables a smooth transition from in-the-clear transmission to encrypted transmission (and its associated technology license) with minimal impact on existing equipment and services.

By allowing simultaneous transmission of in-the-clear and encrypted signals, encryption can be required of broadcasters and receiving equipment, by regulatory authorities (or legislation) on a date certain, without requiring cessation of in the clear transmissions on the same date. Cessation of in the clear transmissions can be set for a date far enough in the future to allow simple obsolescence to minimize the number of legacy receivers that are affected.

Modern digital satellite and broadcast networks often use CA systems that fully encrypt digital audio and video to make programming inaccessible except to those who have properly subscribed. Such encryption is designed to thwart hackers and non-subscribers from receiving programming that has not been paid for, and to provide content handling rules for content after it has been descrambled.

However, terrestrial broadcasts are not currently scrambling their streams. As terrestrial broadcasters wish to protect their content, they are frustrated by the need to support the legacy TVs that are unable to handle scrambled content. Transmitting multiple copies of a single program in the clear and encrypted uses too much bandwidth to be a practical solution, as described earlier.

An embodiment of the present invention addresses this problem by minimizing the bandwidth requirements to provide an equivalent result to multiple carriage without the full bandwidth penalty. The result could be described as "virtual dual carriage" since the benefits of full dual carriage are provided without the full bandwidth cost. A selection criterion is used to select packets for encryption under such a scheme. The criteria used to select packets affect the additional bandwidth requirements and the effectiveness of the encryption.

Certain of the implementations of selective dual carriage described herein utilize an additional (secondary) PID for each duplicated component. These secondary PIDs are used to tag packets that carry duplicated content with the encryption method. The PSI is enhanced to convey information about the existence of these new PIDs in such a way that inserted PIDs are ignored by legacy TVs but can be easily extracted by new TVs.

The new PID is used to tag packets encrypted by the encryption method. Packets with the secondary PID shadow the packets tagged with the primary PID. The packets making up the pairs can occur in either order but, in the preferred implementation, maintain sequence with the clear portion of the PID stream. By use of the primary and secondary PIDs, the decoder located in the set-top box or television set can readily determine which packets are to be decrypted using the decryption method associated with that TV, as will be clear upon consideration of the following description. The processes used to manipulate PIDs will be described later in greater detail.

In general, the encryption technique disclosed herein seeks to encrypt portions of an audio or video signal while leaving other portions of the audio or video signal in the clear to conserve bandwidth. Bandwidth can be conserved because the same clear portion can be sent to all varieties of TVs or other devices. Various methods are used to select the portions of information to be encrypted, for example as described in the above-referenced patent applications. By so doing, the various embodiments of this invention eliminate the traditional "brute-force" technique of encrypting the entire content in one specific scrambling scheme,

which predicates the redundant use of bandwidth if alternate scrambling schemes are desired.

The various embodiments of the invention use several processes, alone or in combination, to send substantial portions of content in the clear while encrypting only a small amount of information required to correctly reproduce the content. Therefore the amount of information transmitted that is encrypted is a small percentage of the content, as opposed to the entire replication of each desired program stream. For purposes of the exemplary systems in this document, the encryption technique described above will now be described in detail.

Substantial efficiency in bandwidth utilization can be achieved by use of a selective packet-by-packet dual carriage. In this technique, packets are selected for duplication and encryption based upon their importance to the proper decompression or enjoyment of the audio and/or video of the program content.

This embodiment can reduce the bandwidth requirement compared with full dual carriage of encrypted content by only scrambling a small fraction of the packets. The original A/V content is left in the clear. Non-legacy TVs share the clear non-duplicated packets, and replace the clear packet with the duplicated packet (marked with a different PID). Non-legacy TVs descramble the encrypted packet. As little as one percent of the total content bandwidth can be duplicated and encrypted. A broadcast station can send the clear content to be received by legacy TVs as before, and a small number of encrypted packets for new TVs.

To decrypt the encrypted packets, the TVs may use a conditional access system such as those used by Motorola, Scientific Atlanta, NDS and others, or may contain some global agreed upon keys.

Referring now to **FIGURE 2**, a block diagram of a system consistent with an exemplary embodiment of the present invention in which portions of programming are dual carried on a packet-by-packet basis. In this system, packets of each program are dual carried using, for example, global agreed upon keys. The packets that are dual carried are selected based upon their importance to the proper decompression or enjoyment of the video and/or audio stream.

In the system illustrated in **FIGURE 2**, the broadcast station 200 selects, duplicates and inserts selected A/V content 201 packets at a processor 202 and encrypts the content at encrypter 203. Packets selected for encryption are chosen so that their non-receipt (by a non-paying decoder) would severely affect the real-time decoding or enjoyment of a program. That is, only critical packets (as defined above) are encrypted. For the video and audio, this can be accomplished, for example, by encrypting "start of frame" transport stream packets containing PES (packetized elementary stream) headers and other headers as part of the payload, since without this information, the STB decoder cannot decompress the MPEG compressed data. MPEG2 streams identify "start of frame" packets with the "Packet Unit Start Indicator" in the transport header. Generally, packets carrying a payload that contains a group of pictures header or a video sequence header can be used to effect the present scrambling technique.

MPEG (Moving Pictures Expert Group) compliant compressed video repackages the elementary data stream into the transport stream in somewhat arbitrary payloads of 188 bytes of data. As such, the transport stream packets containing a PES header can be selected in this example for dual carriage at selector 202 and encrypted by the global keys at the encrypter 203. Packets to be dual carried are duplicated and the PIDs of duplicate packets encrypted by encrypter 202 are remapped at 201 to a secondary PID. The remaining packets are passed in the clear. The clear packets and duplicated and encrypted packets and system information 204 and program specific information 205 are multiplexed together at 208 for broadcast over the broadcast system via antenna 210.

As with the previous system, the legacy TV 215 receives clear packets at antenna 216 and sends them to the tuner 218 and receiver 219 as before. In the new decryption enabled TV 220, the program is received at tuner 222 and receiver 224 via antenna 226 and assigned both a primary and a secondary PID for a single program. The non-duplicated clear packets with the primary PID are received and passed to the decoder. The clear packets (that have been duplicated) are discarded. Encrypted packets with the secondary PID are decrypted at 230and then

recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding.

Using video as an example, each sample is known as a frame and the sample rate is typically 30 frames per second. If the samples are encoded to fit into 3.8 Mbps, each frame would occupy 127K bits of bandwidth. This data is sliced for MPEG transport into packets of 188 bytes with the first packet(s) of each frame containing the header used for instructions to process the body of the frame data. Dual carriage of just the first header packet (1504 additional bits) requires only 1.2% (1504/127K) of additional bandwidth. For high definition (19 Mbps) streams the percentage is even less.

As previously stated, transport stream packets containing a PES header are one preferred target for encryption according to the present embodiment, but other packets could also be selected according to a selection criterion such as those described in the above referenced patent application and others which are pending. These packets contain sequence headers, sequence extension headers, picture headers, quantization and other decode tables that also fall within the same packet. If these packets cannot be decoded by new TVs, not even small portions of the program can be viewed. In general, any attempt by new TVs to tune to the program will likely be met with a blank screen and/or no audio whatsoever since known decoder integrated circuits use the PES header to sync up to an elementary stream such as video and audio in real-time. By encrypting the PES header, the decoding engine in an un-authorized set-top box or TV cannot even get started. Those skilled in the art will appreciate that for implementation of this embodiment of the invention, other critical or important packets or content elements may also be identified for encryption that could severely inhibit unauthorized viewing without departing from the present invention. For example, MPEG intra-coded or I frame picture packets could be encrypted to inhibit viewing of the video portion of the program.

FIGURE 3 is a flow chart depicting an exemplary encoding process such as that which would be used at Broadcast station 200 of **FIGURE 2** starting at 304. Content is received at 308. When a transport stream packet is received at block

202, the packet is examined to determine if it meets a selection criterion for encryption at 312. If not, the packet is passed as a clear unencrypted packet (C) for insertion into the output data stream at 316. If the packet meets the criteria, control passes to 320 and it is duplicated at block 202 to produce a duplicated packet. This encrypted packet is mapped to a secondary PID at block 202. The duplicated packets EA is inserted into the output data stream along with clear packets C at block 202. The duplicated packets are encrypted under global keys at 203 to produce an encrypted packet. Preferably, the duplicated packets are inserted at the location in the data stream where the single original packet was obtained for encryption so that the sequencing of the data remains essentially the same. At 316, the data packets are combined with SI and PSI data and the stream is transmitted at 330.

Thus, a terrestrial broadcast digital television signal consistent with certain embodiments has a collection of modulated packets, with the collection of modulated packets including clear unencrypted packets of content, and duplicates of selected ones of the clear unencrypted packets that are encrypted under an encryption system.

The selective encryption arrangement described above can greatly reduce the bandwidth requirements over that required for full dual carriage. Encrypting the PES header information can be effective in securing video and audio content, while allowing content to also be received in the clear by legacy TVs in the same broadcast system. Legacy TVs are un-affected, and new TVs require only an minor hardware, firmware, or software enhancement to listen for two PIDs each for video and audio. Broadcast station modification is limited to selecting content for dual carriage, encrypting the duplicated packet, and providing a means to mix the duplicated packet into a composite output stream.

The PID mapping concepts described above can be generally applied to the selective dual carriage techniques described herein, where needed. At the broadcast station, the data stream of packets is manipulated to duplicate packets selected for dual carriage. Those packets are sent in two distinct encryption manners – clear and encrypted. The duplicated packets are assigned separate PIDs

(one of which matches the reset of the clear content) and reinserted in the location of the original selected packet in the data stream for transmission over the broadcast system. At the output of the broadcast system, a stream of packets appears with global key encrypted packets, and clear packets having a different PID. A secondary PID identifies the packets that are encrypted under the encryption system. In addition to the PID remapping that takes place at the station, MPEG packets utilize a continuity counter to maintain the appropriate sequence of the packets. In order to assure proper decoding, this continuity counter should be properly maintained during creation of the packetized data-stream at the station. This is accomplished by assuring that packets with each PID are assigned continuity counters sequentially in a normal manner. Thus, packets with the secondary PID will carry a separate continuity counter from those of the primary PID. This is illustrated below in simplified form where PID 025 is the primary PID and PID 125 is the secondary PID, E represents an encrypted packet, C represents a clear packet, and the end number represents a continuity counter.

025C04	025C05	125E11	025C06	025C07	025C08	025C09	125E12

In this exemplary segment of packets, packets with PID 025 are seen to have their own sequence of continuity counters (04, 05, 06, 07, 08, 09, ...). Similarly, the packets with secondary PID 125 also have their own sequence of continuity counters (11, 12, ...).

At the STB, the PIDs can be manipulated in any number of ways to correctly associate the encrypted packets with secondary PID with the correct program. In one implementation, the packet headers of an input stream segment illustrated below:

025C04	025C05	125E11	025C06	025C07	025C08	025C09	025E10

are manipulated to create the following output stream segment:

125C04	025E11	125C05	125C06	125C07	125C08	125C09	125E10

The primary PIDs (025) in the input stream are replaced with the secondary PID (125) for the clear packets (C). For the encrypted packets, the primary PID and secondary PID are retained, but the continuity counters are swapped. Thus, the stream of packets can now be properly decrypted and decoded without errors caused by loss of continuity using the secondary PID. Other methods for manipulation of the PIDs, e.g. mapping the PID (125) on the duplicated clear packet to a NOP PID (all ones) or other PID value not decoded, and the continuity counters can also be used in embodiments consistent with the present invention.

The primary and secondary PIDs are conveyed to the STBs in the program map table (PMT) transmitted as a part of the program system information (PSI) data stream. The existence of a secondary PID can be established to be ignored by the TV operating without descrambling capability. But new TVs operating with knowledge of the global ATSC keys are programmed to recognize that secondary PIDs are used to replace the clear part of the program associated with the primary PID. The set-top boxes are alerted to the fact that this encryption scheme is being used by the presence of a ATSC CA descriptor in the elementary PID "for loop" of the PMT. There typically would be a CA descriptor for the video elementary PID "for loop", and another one in the audio elementary PID "for loop". The CA descriptor uses a Private Data Byte to identify the CA_PID as either the ECM PID or the secondary PID used for selective scrambling, thus setting up the STB operating under system B to look for both primary and secondary PIDs associated with a single program. Since the PID field in the transport header is thirteen bits in length, there are 2^{13} or 8,192 PIDs available for use, any spare PIDs can be utilized for the secondary PIDs as required.

While conceptually the PID mapping at the broadcast station is a simple operation, in practice the broadcast station equipment is often already established and is therefore modified to accomplish this task in a manner that is minimally disruptive to the established broadcast system while being cost effective. Thus, the details of the actual implementation within the broadcast system are somewhat

dependent upon the actual legacy hardware present in the station, examples of which are described in greater detail below.

Several TV implementations are possible within the scope of the present invention. The method used at the headend to select packets for encryption is irrelevant to the STB.

One such implementation is illustrated in **FIGURE 4**. In this embodiment, packets are received by an antenna and passed to a tuner and demodulator 404. Packets are then provided to a decoder circuit 408's demultiplexer 410. The packets are buffered into a memory 412 (e.g., using a unified memory architecture) and processed by the STB's main CPU 416 (or other CPU or hardware) using software or firmware stored in memory 412.

Selected PIDs can be stripped from the incoming transport via the STB's PID filter, decrypted and buffered in SDRAM, similar to the initial processing required in preparation for transfer to an HDD in a PVR application. The host CPU 916 can then "manually" filter the buffered data in SDRAM for elimination of the packets containing unneeded PIDs. There are some obvious side effects to this process.

An exemplary process 500 for carrying out the decoding of received content is illustrated in **FIGURE 5** starting at 504. Content is received at 508 and passed to 512 where a determination is made as to whether the content is secondary (i.e., encrypted and identified by a secondary PID). If not, the content is sent directly to the decoder at 516. If so, the duplicate packets carrying the primary (unencrypted) content is dropped at 520 and the secondary content is decrypted at 524. Content is then passed to the decoder at 516, and the content is decoded at 530.

The host overhead is estimated to be about 1% of the bandwidth of the CPU. In the worst case, this is equivalent to 40K bytes/Second for a 15 Mbit/S video stream. This reduction is possible since at most only 4 bytes of each packet is evaluated and the location is on 188 byte intervals so the intervening data does not have to be considered. Each packet header in SDRAM can therefore be directly accessed through simple memory pointer manipulation. Additionally,

Packets are cached in blocks and evaluated en masse to reduce task switching of the host. This would eliminate an interrupt to other tasks upon the reception of each new packet. This may produce a increased latency for starting decode of a stream upon channel change to allow time for cache fill. This may be negligible depending upon the allocated SDRAM cache buffer size.

The host filtered packets in the SDRAM buffer are then transferred to the A/V Queue through existing hardware DMA processes and mimics a PVR implementation. The filtered packets are then provided to the decoder 922 for decoding.

The present embodiments have been described in terms of a digital A/V system using MPEG 2 coding. Thus, the various packet names and protocol specifically discussed is related the MPEG 2 coding and decoding. However, those skilled in the art will appreciate that the concepts disclosed and claimed herein are not to be construed in such a limited scope. The same or analogous techniques can be used in any digital broadcast system without limitation to MPEG 2 protocols.

Also, while the present invention has been described in terms of the use of the encryption and copy protection techniques described to provide a mechanism for dual carriage of a television program, those skilled in the art will appreciate that the concepts disclosed and claimed herein are not to be construed in such a limited scope. The same or analogous techniques can be used in any digital transmission system without limitation to television protocols.

Additionally, although specifically disclosed for the purpose of encrypting and copy protecting television programming, the present inventions can be utilized for dual carriage of other content including, but not limited to content for download over the Internet or other network, music content, packaged media content as well as other types of information content. Such content may be played on any number of playback devices including but not limited to personal digital assistants (PDAs), personal computers, personal music players, audio systems, audio / video systems, etc. without departing from the present invention that do not have descrambling capability.

Numerous embodiments are possible without departing from the present invention. For example, a method of encrypting a digital television signal, consistent with certain embodiments of the invention may involve examining unencrypted packets of data in the digital television signal to identify a selected packet type; duplicating packets identified as being of the selected packet type; encrypting the duplicated packets; and adding the duplicated and encrypted packets along with the unencrypted packets of the selected packet type in the digital television signal to produce a selectively encrypted digital television signal. The method can further involve distributing an ATSC broadcast flag with the selectively encrypted digital television signal. The content can represent one or more channels in a transport stream, regardless of whether other channels are encrypted or unencrypted. In addition, the key used to encrypt the content can be a function of the copy control information of the content, or the key used to encrypt the content can be a function of global ATSC defined keys. The selected packet type may be, for example, a packet carrying information that is needed to decompress the digital television signal. The method can further involve assigning a packet identifier to the unencrypted packets. The method can further involve assigning the packet identifier to the encrypted packets. The packet identifier can be a primary packet identifier; and a secondary packet identifier can be assigned to the encrypted packets.

In another exemplary embodiment, a method of encrypting a digital television signal involves examining unencrypted packets of data in the digital television signal to identify a selected packet type; identifying packets as being of the selected packet type to produce first packets; duplicating and encrypting the packets identified as being of the selected packet type using an encryption method to produce second packets; and replacing the unencrypted packets of the selected packet type with the first packets and the second packets in the digital television signal to produce a selectively dual encrypted television signal. The method can further involve assigning a packet identifier to the unencrypted packets. The method can further involve assigning the packet identifier to the encrypted packets.

A television receiver, consistent with certain embodiments of the present invention has a receiver receiving a digital television signal. The signal has a plurality of unencrypted packets; and a plurality of encrypted packets, wherein the encrypted packets duplicate some of the unencrypted packets and contain information required to decode the digital television signal. A decrypter decrypts the encrypted packets and drops the transmitted unencrypted version of the same packets. A decoder decodes the unencrypted packets and the decrypted packets to produce a signal suitable for play on a television set. In certain embodiments, the digital television signal complies with an MPEG standard, and the unencrypted packets are identified by a primary packet identifier, and the encrypted packets are identified by a secondary packet identifier. In certain embodiments, the digital television signal is compressed, and the encrypted packets comprises a packet type that is needed to decompress the digital television signal if the duplicated packets sent in the clear are ignored.

In other embodiments consistent with the invention, a method of decoding a selectively encrypted television program, involves receiving a digital television program comprising a plurality of packets, wherein certain packets of the plurality of packets are encrypted and a remainder of the packets are unencrypted, wherein the encrypted packets are also sent unencrypted and contain information that is required for correct decoding of the television program; decrypting the encrypted packets to produce decrypted packets; and decoding the decrypted packets and the unencrypted packets to produce a decoded television signal. In certain embodiments, the selectively encrypted television program is a digital television program, and the certain encrypted packets comprise packets that are needed to decode the television program if the duplicated packets sent in the clear are ignored. In certain embodiments, the selectively encrypted television program complies with a digital satellite service or digital cable transport standard, and wherein the encrypted packets carry a payload of a packetized elementary stream header.

In other embodiments, a method of decoding selectively encrypted content involves receiving selectively encrypted content comprising unencrypted content,

content sent in the clear and encrypted under an encryption system, the encrypted content comprising information needed for correct decoding of the selectively encrypted content if the duplicated content in the clear is ignored; and decrypting the encrypted content under the encryption system to produce decrypted content. In certain embodiments, the method further involves decoding the unencrypted content, ignoring the duplicated unencrypted content, and the decoding decrypted content to decode the selectively encrypted content. In other embodiments, the digital television signal complies with a digital satellite service or digital cable transport standard, and wherein the encrypted packets carry a payload of a packetized elementary stream header.

It should be understood that terrestrial broadcasts signals not only emanate over-the-air, but also be part of satellite "local-into-local" and cable "must carry" content offerings. For those delivery options, the streams as encoded by certain embodiments consistent with the present invention can be passed through to the satellite or cable set-top box for processing in a similar fashion as the new TV. Another possibility, is that copy protection information can be "transcoded" into the satellite or cable format with the result that the content is 100% encrypted using the conditional access provider of the satellite or cable system. The set-top boxes in those systems could obey the copy protection rules that would be "transcoded' from the original terrestrial broadcast signal.

Those skilled in the art will recognize that the present invention has been described in terms of exemplary embodiments that can be realized by use of a programmed processor. However, the invention should not be so limited, since the present invention could be implemented using hardware component equivalents such as special purpose hardware and/or dedicated processors which are equivalents to the invention as described and claimed. Similarly, general purpose computers, microprocessor based computers, micro-controllers, optical computers, analog computers, dedicated processors and/or dedicated hard wired logic may be used to construct alternative equivalent embodiments of the present invention.

Thus, an encryption arrangement for television programs or other digital programming consistent with certain embodiments sends content completely in-

the-clear and also encrypts only a portion of the content required for full presentation of a television program. The arrangement allows interoperability between new TVs that can handle encryption and older TVs that cannot. Regulations prevent new TVs from receiving only the clear content. New TVs are made to descramble the encrypted portions of the content. Older legacy TVs can receive all the content in the clear. The encrypted portions are chosen so that dramatically less bandwidth is required as compared to full dual carriage of the content. Licensing provisions relating to the encryption technology can be used to control unauthorized use of content.

Those skilled in the art will appreciate that the program steps and associated data used to implement the embodiments described above can be implemented using disc storage as well as other forms of storage such as for example Read Only Memory (ROM) devices, Random Access Memory (RAM) devices; optical storage elements, magnetic storage elements, magneto-optical storage elements, flash memory, core memory and/or other equivalent storage technologies without departing from the present invention. Such alternative storage devices should be considered equivalents.

The present invention, as described in embodiments herein, can be implemented using a programmed processor executing programming instructions that are broadly described above in flow chart form that can be stored on any suitable electronic storage medium or transmitted over any suitable electronic communication medium. However, those skilled in the art will appreciate that the processes described above can be implemented in any number of variations and in many suitable programming languages without departing from the present invention. For example, the order of certain operations carried out can often be varied, additional operations can be added or operations can be deleted without departing from the invention. Error trapping can be added and/or enhanced and variations can be made in user interface and information presentation without departing from the present invention. Such variations are contemplated and considered equivalent.

While the invention has been described in conjunction with specific embodiments, it is evident that many alternatives, modifications, permutations and variations will become apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended that the present invention embrace all such alternatives, modifications and variations.

What is claimed is: